

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-051442

(43)Date of publication of application : 20.02.1998

(51)Int.Cl.

H04L 9/32
G09C 1/00

(21)Application number : 08-207266

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 06.08.1996

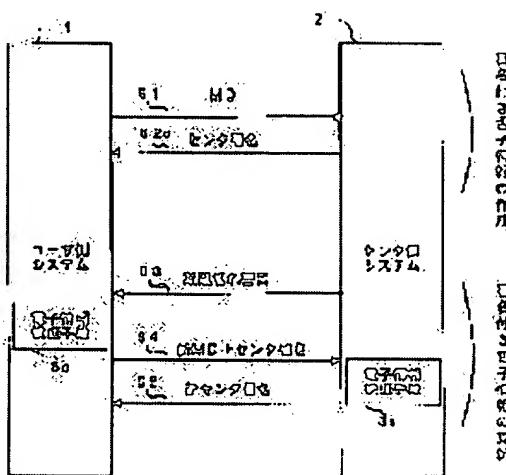
(72)Inventor : KOBAYASHI NOBUHIRO

(54) ELECTRONIC SIGNATURE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic information signature method suitable for verification of a document over a long period with a small quantity of signature information.

SOLUTION: A user side system 1 sends a message digest(MD) generated based on electronic information in the user side system 1 to a center side system 2 (step S1). The center side system 2 sends a center signature generated by applying electronic signature to the received MD through the use of a 1st center secret key to the user side system 1 (step S2a). Thus, electronic information with signature is generated. In the case of updating the electronic information with signature, an electronic information verification means 3a verifies the validity of the electronic information with signature. When the information is discriminated to be valid as the result of verification, a new MD is sent to the center side system 2 (step S4) and the new center signature is received in the step 5.



LEGAL STATUS

[Date of request for examination] 20.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-51442

(43)公開日 平成10年(1998)2月20日

(51) Int.Cl. ⁸	識別記号	序内整理番号	F I	技術表示箇所
H 04 L 9/32			H 04 L 9/00	6 7 5 B
G 09 C 1/00	6 4 0	7259-5 J 7259-5 J	G 09 C 1/00	6 4 0 B 6 4 0 D
			H 04 L 9/00	6 7 5 D

審査請求 未請求 請求項の数 6 O L (全 23 頁)

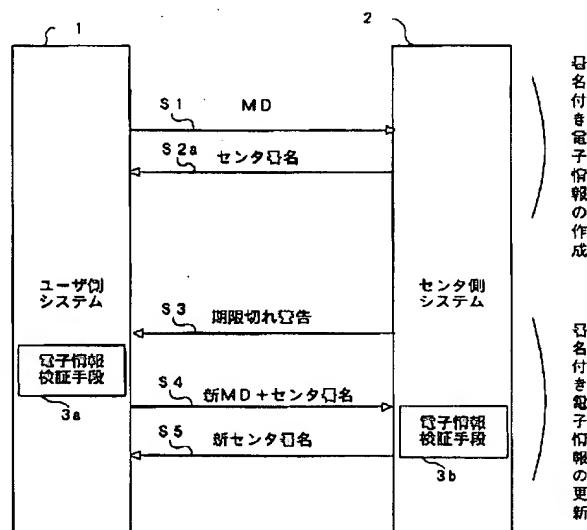
(21)出願番号	特願平8-207266	(71)出願人	000006013 三菱電機株式会社 東京都千代田区丸の内二丁目2番3号
(22)出願日	平成8年(1996)8月6日	(72)発明者	小林 信博 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
		(74)代理人	弁理士 宮田 金雄 (外3名)

(54)【発明の名称】 電子署名方法

(57)【要約】

【課題】 少ない署名情報で長期間にわたって電子情報の安全性を保つことができない。

【解決手段】 ユーザ側システム1が、ユーザ側システム1内の電子情報に基づいて生成されたMDをセンタ側システム2へ送信する(ステップS1)。センタ側システム2が、受信したMDを第1のセンタ秘密鍵を用いて電子署名することにより生成したセンタ署名をユーザ側システム1へ送信する(ステップS2a)。以上により、署名付き電子情報を生成する。この署名付き電子情報を更新する際には、電子情報検証手段3aが署名付き電子情報の正当性を検証する。検証の結果、正当であると判断された場合には、センタ側システム2へ新MDを送信し(ステップS4)、ステップ5で新センタ署名を受け取る。



【特許請求の範囲】

【請求項1】 第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより生成した第1の署名情報を上記第1のシステムへ送信する第2の送信ステップと、

上記第1のシステムが、上記第1の署名情報を記憶する第1の記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第1の記憶ステップで記憶された第1の署名情報を用いて上記電子情報が正当であるか否かを検証する検証ステップと、

この検証ステップの検証結果が正当であると判断された場合に上記第1のシステムが、上記第1の情報を上記第2のシステムへ送信する第3の送信ステップと、

上記第2のシステムが、上記第3の送信ステップで送信された第1の情報を第2の秘密鍵を用いて署名することにより生成された第2の署名情報を上記第1のシステムへ送信する第4の送信ステップと、

上記第1のシステムが、上記第2の署名情報を記憶する第2の記憶ステップと、を備えた電子署名方法。

【請求項2】 第1の情報は、電子情報を第3の秘密鍵を用いて署名することにより生成した第3の署名情報に基づいて生成され、

検証ステップは、第1の署名情報又は上記第3の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第1の署名情報及び第3の署名情報を用いて上記電子情報が正当であるか否かを検証することを特徴とする請求項1に記載の電子署名方法。

【請求項3】 第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより生成した第1の署名情報を上記第1のシステムへ送信する第2の送信ステップと、

上記第1のシステムが、上記第1の署名情報を記憶する記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第1の情報を上記第2のシステムへ送信する第3の送信ステップと、

上記第2のシステムが、上記第1の署名情報を用いて上記第1の情報が正当であるか否かを検証する検証ステップと、

上記第1の検証ステップの検証結果が正当であると判断された場合に上記第2のシステムが、上記第1の情報を第2の秘密鍵を用いて署名することにより生成された第2の署名情報を送信する第4の送信ステップと、

10

上記第1のシステムが、上記第2の署名情報を記憶する第2の記憶ステップと、を備えた電子署名方法。

【請求項4】 上記電子情報を第3の秘密鍵を用いて署名することにより生成した第3の署名情報又は上記第1の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第3の署名情報を用いて上記電子情報が正当であるか否かを検証する第2の検証ステップを備え、

上記第1の情報は、上記第3の署名情報に基づいて生成され、

上記第3の送信ステップは、上記第2の検証ステップの検証結果が正当であると判断された場合に上記第1のシステムが、上記第1の情報を代えて、上記電子情報を第4の秘密鍵を用いて電子署名することにより生成した第4の署名情報に基づいて生成した第2の情報を上記第2のシステムへ送信し、

上記第1の検証ステップは、上記第2のシステムが、上記第1の署名情報を用いて上記電子情報が正当であるか否かを検証し、

上記第4の送信ステップは、上記第1の検証ステップの検証結果が正当であると判断された場合に上記第2のシステムが、上記第1の情報を代えて上記第2の情報を第2の秘密鍵を用いて電子署名することにより生成された第2の署名情報を送信することを特徴とする請求項3に記載の電子署名方法。

【請求項5】 第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、

上記第1の情報と上記第1の署名情報を上記第2のシステムに記憶する第1の記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第2のシステムが、上記第1の情報を第2の秘密鍵で電子署名することにより第2の署名情報を生成する第2の生成ステップと、

上記第2の署名情報を記憶する第2の記憶ステップと、を備えた電子署名方法。

【請求項6】 第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、

上記第1の情報と上記第1の署名情報を上記第2のシステムに記憶する第1の記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第2のシステムが、上記第1の署名情報を第2の秘密鍵を用いて電子署名することにより第2の署名情報を生

40

50

3

成する第2の生成ステップと、
上記第2の署名情報を上記第2のシステムに記憶する第
2の記憶ステップと、を備えた電子署名方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電子情報に電子
署名を付加しその電子署名を認証する電子署名方法に関する。

【0002】

【従来の技術】図12は特開平7-5809号公報に示された
従来の文書の署名装置を説明する機能ブロック図である。
図12において、30はユーザの作成した文書、31は文書30を走査しその画像信号を出力する走査器、
32は走査器31が output した画像信号をデジタル形式に
変換し第1の信号として出力するA/D変換器、33は
第1の信号を圧縮する圧縮器、E1は暗号化に用いる暗号
化鍵、35は圧縮された第1の信号を暗号化鍵E1を用いて
暗号化し第2の信号を生成する暗号器、E1[Di]は暗号
化鍵E1に対応する解読鍵Diを暗号化鍵E1で暗号化した暗
号済解読鍵、37は第2の信号に暗号化された解読鍵E1
[Di]を付与して所定のフォーマットに従って符号化する
符号器、38は暗号器35の使用する暗号化鍵E1と符号
器37の使用する解読鍵E1[Di]を送るセンター、39は
符号化された情報から生成され文書30に添付される署
名ラベル、40は符号器37により符号化された情報から
署名ラベルLを生成する符号発生器である。

【0003】次に動作について説明する。この署名装置は、文書30の画像信号を走査して、この文書30の変造防止用の署名ラベルLを生成するものである。まず、走査器31は文書30を走査し、その文書30の画像信号を出力する。A/D変換器32はこの画像信号を受け取り、デジタル形式に変換し、第1の信号として出力する。圧縮器33は第1の信号を圧縮して暗号器35へ出力する。この圧縮は署名ラベルLに記憶するデータの量を減少させるために行われる。暗号器35は周知のRSA方式のような公開鍵暗号方式のための暗号化鍵E1を用いて第1の信号を暗号化し、この暗号化した信号を第2の信号として出力する。この際、鍵の解読を防ぐ為に十分に長い鍵E1を用いる。暗号化された第2の信号は符号器37によりある所定のフォーマットに従って符号化される。そして、符号器37は符号発生器40を制御して符号化された署名ラベルLを生成させる。この署名ラベルLは文書30に添付されるものである。この際、第2の信号の解読を容易にするために、符号器37により暗号化された解読鍵E1[Di]を第2の信号に付加する。なお、暗号化鍵E1および暗号化された解読鍵E1[Di]はセンタ38から送られる。

【0004】そして、この署名装置によって生成された
署名ラベルLは、文書30の第1の信号に付加され、図
示しないラベル付きの文書LDとして保存される。ラベ
ル付き文書LDを認証する際には、当該文書LDの第1
の信号（画像表現部分）と署名ラベルLを比較すること
により、文書30が変造されているか否かが判断でき
る。すなわち、第1の信号を改変したとしても、暗号鍵
E1を用いない限り署名ラベルLを変更することはでき
ず、第1の信号と署名ラベルLとを一致させることはで
きないからである。

4

ル付き文書LDを認証する際には、当該文書LDの第1
の信号（画像表現部分）と署名ラベルLを比較すること
により、文書30が変造されているか否かが判断でき
る。すなわち、第1の信号を改変したとしても、暗号鍵
E1を用いない限り署名ラベルLを変更することはでき
ず、第1の信号と署名ラベルLとを一致させることはで
きないからである。

【0005】

【発明が解決しようとする課題】上述のような従来の署
名装置は以上のように構成されているため、署名が解読
されない為に長い鍵を用いて署名情報を作成しなければ
ならず、元の文書に多量の情報を追加することが必要で
あるという問題があった。

【0006】また、所定の満定期限で署名情報の更新
し、署名情報の量を少なくする場合では、各期限内にお
いて文書が変更されていないことが認証できるのみであ
り、長期に渡って文書が変更されていないことが認証で
きなかった。

【0007】この発明は、かかる問題点を解決するため
になされたもので、署名情報の量が少なく、長期に渡る
文書の認証に適した電子情報署名方法を得ることを目的
とする。

【0008】

【課題を解決するための手段】この発明にかかる電子署
名方法においては、第1のシステムが、第1のシステム
内の電子情報に基づいて生成された第1の情報を第2の
システムへ送信する第1の送信ステップと、第2のシス
テムが、受信した第1の情報を第1の秘密鍵を用いて電
子署名することにより生成した第1の署名情報を第1の
システムへ送信する第2の送信ステップと、第1のシス
テムが、第1の署名情報を記憶する第1の記憶ステップ
と、第1の署名情報の有効期限に基づいた更新時期に第
1のシステムが、第1の記憶ステップで記憶された第1
の署名情報を用いて電子情報が正当であるか否かを検証
する検証ステップと、この検証ステップの検証結果が正
当であると判断された場合に第1のシステムが、第1の
情報を第2のシステムへ送信する第3の送信ステップ
と、第2のシステムが、第3の送信ステップで送信され
た第1の情報を第2の秘密鍵を用いて署名することによ
り生成された第2の署名情報を第1のシステムへ送信す
る第4の送信ステップと、第1のシステムが、第2の署
名情報を記憶する第2の記憶ステップと、を備えたもの
である。

【0009】また、第1の情報は、電子情報を第3の秘
密鍵を用いて署名することにより生成した第3の署名情
報に基づいて生成され、検証ステップは、第1の署名情
報又は第3の署名情報の有効期限に基づいた更新時期に
第1のシステムが、第1の署名情報及び第3の署名情報
を用いて電子情報が正当であるか否かを検証することを
特徴とするものである。

【0010】また、第1のシステムが、第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、第2のシステムが、受信した第1の情報を第1の秘密鍵を用いて電子署名することにより生成した第1の署名情報を第1のシステムへ送信する第2の送信ステップと、第1のシステムが、第1の署名情報を記憶する記憶ステップと、第1の署名情報の有効期限に基づいた更新時期に第1のシステムが、第1の情報を第2のシステムへ送信する第3の送信ステップと、第2のシステムが、第1の署名情報を用いて第1の情報が正当であるか否かを検証する検証ステップと、第1の検証ステップの検証結果が正当であると判断された場合に第2のシステムが、第1の情報を第2の秘密鍵を用いて署名することにより生成された第2の署名情報を送信する第4の送信ステップと、第1のシステムが、第2の署名情報を記憶する第2の記憶ステップと、を備えたものである。

【0011】また、電子情報を第3の秘密鍵を用いて署名することにより生成した第3の署名情報又は第1の署名情報の有効期限に基づいた更新時期に第1のシステムが、第3の署名情報を用いて電子情報が正当であるか否かを検証する第2の検証ステップを備え、第1の情報は、第3の署名情報に基づいて生成され、第3の送信ステップは、第2の検証ステップの検証結果が正当であると判断された場合に第1のシステムが、第1の情報に代えて、電子情報を第4の秘密鍵を用いて電子署名することにより生成した第4の署名情報に基づいて生成した第2の情報を第2のシステムへ送信し、第1の検証ステップは、第2のシステムが、第1の署名情報を用いて電子情報が正当であるか否かを検証し、第4の送信ステップは、第1の検証ステップの検証結果が正当であると判断された場合に第2のシステムが、第1の情報に代えて第2の情報を第2の秘密鍵を用いて電子署名することにより生成された第2の署名情報を送信することを特徴とするものである。

【0012】また、第1のシステムが、第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、第2のシステムが、受信した第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、第1の情報と第1の署名情報を第2のシステムに記憶する第1の記憶ステップと、第1の署名情報の有効期限に基づいた更新時期に第2のシステムが、第1の情報を第2の秘密鍵で電子署名することにより第2の署名情報を生成する第2の生成ステップと、第2の署名情報を記憶する第2の記憶ステップと、を備えたものである。

【0013】また、第1のシステムが、第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、第2のシス

テムが、受信した第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、第1の情報と第1の署名情報を第2のシステムに記憶する第1の記憶ステップと、第1の署名情報の有効期限に基づいた更新時期に第2のシステムが、第1の署名情報を第2の秘密鍵を用いて電子署名することにより第2の署名情報を生成する第2の生成ステップと、第2の署名情報を第2のシステムに記憶する第2の記憶ステップと、を備えたものである。

【0014】

【発明の実施の形態】

実施の形態1. 図1は、この発明の実施の形態1における電子情報署名システムのデータの流れを説明するシーケンス図である。この図1に示した電子情報署名システムは、文字、画像データ等からなる契約書等の電子情報の改変、偽造等を防止するシステムであり、1は電子情報を有する第1のシステムたるユーザ側システム、2は複数のユーザ側システム1が接続され、ユーザ側システム1の要求に応じて電子情報に署名を行う第2のシステムたるセンタ側システムである。3aはユーザ側システム1に設けられたこの発明の特徴的な部分の1つである電子情報検証手段であり、電子情報が改変されていないかを検証し、改変されていないことを確認した場合に署名を更新する働きがある。同様に、3bはセンタ側システム2に設けられたこの発明の特徴的な部分の1つである電子情報検証手段であり、電子情報が改変されていないかを検証し、改変されていないことを確認した場合に署名を更新する働きがある。

【0015】次に、図1を用いて動作の概要を説明する。まず、第1の送信ステップとして、ステップS1で、ユーザ側システム1は、センタ側システム2の署名を得るために、自己の有する電子情報のメッセージダイジェスト（以下、MDと略す）を送信する。このMDは第1の情報である。MDは電子情報から1方向性関数によって生成される電子情報の要約であり、MDから電子情報の内容を知ることはできない。ただし、電子情報が改変されるとMDも変化するため、MDに基づいて改変されているか否かの判断は可能となっている。従って、センタ側システムに電子情報の内容を公開することなく、署名を受けることができる。第1の情報としては、例えば、電子情報を周知のデータ圧縮技術によって圧縮したもの、又は電子情報そのものを用いてよい。

【0016】次に第2の送信ステップとして、ステップS2aで、MDを受け取ったセンタ側システム2は、このMDから第1の署名情報を有するセンタ署名を生成し、ユーザ側システム1に送信する。署名は、MDをセンタのみが知っている第1の秘密鍵たる秘密鍵で暗号化したものであり、MDが変わると生成される署名も変わらようになっている。このセンタ署名を受け取ったユーザ側システム1は、第1の記憶ステップとして、電子情報、電

7

子情報をユーザ側システム1のみが知っている秘密鍵を用いて生成したユーザ署名、及びセンタ側システム2から送信されたセンタ署名という3つの情報をまとめて署名付き電子情報として記憶する。この署名付き電子情報は、上述のようにユーザ側システム1及びセンタ側システム2の署名を含むため、ユーザ側システム1、あるいはセンタ側システム2の一方が電子情報を改変しようとしても、他方のシステムの署名を改変することができない。そのため、電子情報とユーザ署名、電子情報から生成したMDとセンタ署名との整合性を調べることにより不正を検出し、改変、偽造等を防止することができる。

【0017】以上で、署名付き電子情報の生成が終了する。しかし、ユーザ署名及びセンタ署名はそれぞれ秘密鍵によって暗号化された情報であり、多量の計算を行うことにより秘密鍵が解読される可能性がある。この問題を解決する方法として、容易に解読できない長さの署名を行う方法がある。しかし、この方法では署名付き電子情報のデータ量が多くなってしまうという別の問題が発生し、また解読不可能な期間が有限であるという問題がある。この発明では署名に期限を設け、署名の長さをこの期限内に解読できないような長さとすることにより、署名のデータ量を減らすことができる。

【0018】上述の期限を過ぎた署名は無効とされ、署名としての効力を持たないため、期限毎に署名を更新する必要がある。以下に、この更新処理の概要を説明する。まず、ステップS3で、センタ側システム2が内部に記憶した期限を参照し、期限切れが近づくと期限切れ警告を送信する。

【0019】次に、検証ステップとして、ステップS4で、期限切れ警告を受け取ったユーザ側システム1が、電子情報検証手段3aにより、ユーザ側システム1に記憶した署名付き電子情報の検証を行う。検証の結果、電子情報が改変されていないことが判明した場合には、第3の送信ステップとして、電子情報のMDとこのMDに対応するセンタ署名を送信する。

【0020】続いて、ステップS5で、MD及びセンタ署名を受け取ったセンタ側システム2が、電子情報検証手段3bにより受け取ったMDとセンタ署名とを用いてセンタ署名を検証する。検証の結果、センタ署名が正当であることを確認した場合には、第4の送信ステップとして、第2の秘密鍵たる新たな秘密鍵とMDを用いて、第2の署名情報を新センタ署名を生成しユーザ側システム1へ送信する。

【0021】次に、第2の記憶ステップとして新センタ署名を受け取ったユーザ側システム1では、この新センタ署名、ユーザ署名、及び電子情報をまとめて署名付き電子情報として記憶する。以上により、署名付き電子情報の更新が終了する。以降は、期限切れが近づく度に更新を繰り返す。

【0022】以上に示した電子情報署名システムによれ

10

20

30

40

50

8

ば、電子情報の改変を少ないデータ量で長期間に渡って防止することができる。特に、署名の更新時に電子情報若しくは署名の正当性を検出し、正当であるときに署名付き電子情報の更新を行ふため、現在の署名が正当であれば、過去における複数の期間に渡って電子情報が改変されていないことが保証される。一方、更新時に機能する電子情報検証手段3a、bを持たない従来のシステムでは、更新時に電子情報が書き換えられる可能性があり、長期にわたって電子情報が改変されていないことを保証できない。

【0023】◆システム詳細

次に、図1に示した電子情報検証システムのより詳細な実施の形態について説明する。図2は図1に示した電子情報検証システムの署名付き電子情報の作成処理を説明する機能ブロック図、図3は同様に署名付き電子情報の更新時における検証処理、図4も同様に署名付き電子情報の更新処理をそれぞれ説明する機能ブロック図である。

【0024】図2において、図1と同一の符号は同一又は相当の部分を表す。i1aは署名付すべき電子情報、Suはユーザ側システム1が外部に対して秘密に保管する公開鍵暗号方式におけるユーザ秘密鍵、4は電子情報i1aをユーザ秘密鍵Suを用いて暗号化し、ユーザ署名i2aを生成するユーザ署名手段、5はユーザ署名i2aを受け付け、このユーザ署名i2aを一方向性関数（メッセージ要約関数とも呼ばれる）により要約しMDi3として出力するMD生成手段である。Scはセンタ側システム2が外部に対して秘密に保管する公開鍵暗号方式におけるセンタ秘密鍵、i4はセンタ秘密鍵Scの解読の容易性に応じて定められ、センタ署名i5aの有効な日時を表す有効期限、6はユーザ署名i2aが送信したMDi3及び有効期限i4をセンタ秘密鍵Scを用いて暗号化し、センタ署名i5aとして出力するセンタ署名手段、7は有効期限i4を記憶する有効期限保管手段である。11は電子情報i1a、ユーザ署名i2a、及びセンタ側システム2が送信したセンタ署名i5aをまとめて1つの情報とし、この情報を署名付き電子情報i6aとして出力する署名付き電子情報生成手段である。

【0025】・署名付き電子情報作成処理

次に、図2を用いて署名付き電子情報i6aの作成処理動作について説明する。まず、ユーザ側システム1において、ユーザ署名手段4は電子情報i1aを暗号化し、第3の署名情報を用いて新センタ署名i2aを生成する。この暗号化は第3の秘密鍵たるユーザ秘密鍵Suを用いて、例えばRSA方式のような公開鍵暗号方式によって行われる。MD生成手段5はユーザ署名i2aを受け取り、このユーザ署名i2aを基にMDi3を生成する。MDi3は上述のように一方向性関数を用いてユーザ署名i2aを要約し、データ量を少なくした情報となってい

る。MD生成手段5によって生成されたMD i 3はセンタ側システム2に送信される。

【0026】MD i 3を受け取ったセンタ側システム2では、センタ署名手段6がMD i 3及び有効期限i 4をセンタ秘密鍵S cを用いて暗号化しセンタ署名i 5 aを生成する。暗号化は、上述ユーザ署名手段4と同様に、例えばRSA方式のような公開鍵暗号方式を用いて行う。また、有効期限i 4はセンタ署名i 5 aの作成時からセンタ署名i 5 aの解読が困難な期間を指定して生成され、有効期限保管手段7に保管される。そして、センタ側システム2は生成したセンタ署名i 5 aとその有効期限i 4をユーザ側システム1へ送信する。

【0027】ユーザ側システム1では、センタ署名i 5 aとその有効期限i 4を受け取ると、電子情報i 1 a、ユーザ署名i 2 a、有効期限i 4及びセンタ署名i 5 aを1つの情報にまとめ、署名付き電子情報i 6 aを生成する。この署名付き電子情報i 6 aの生成は、署名付き電子情報生成手段11が行う。そして、ユーザ側システム1にこの署名付き電子情報i 6 aを記憶する。以上で、署名付き電子情報i 6 aの作成処理が完了する。

【0028】・署名付き電子情報更新処理

続いて、図3及び4を用いて署名付き電子情報i 6 aの更新処理を説明する。まず、更新時の検証処理について図3を用いて説明する。図3は検証処理時の電子情報署名システムの動作を説明する機能ブロック図である。図3において、図1又は図2と同一の符号は同一又は相当の部分を表している。8 aはMD生成手段5より再生成MD i 8、署名付き電子情報i 6 a内に記憶されているセンタ署名i 5 b、及び有効期限i 4 bを受け取り、この3つの情報とセンタ公開鍵P cとを用いてセンタ署名が正当であるかを検証するセンタ署名検証手段である。ここで、センタ署名i 5 b、有効期限i 4 bは、それぞれ電子情報作成時に記憶されたセンタ署名i 5 a、有効期限i 4に相当するものであり、センタ署名が改変されなければセンタ署名i 5 a、有効期限i 4と同一の情報である。また、センタ公開鍵P cは、センタ秘密鍵S cに対応する復号のための鍵であり、センタ秘密鍵S cを生成したセンタ側システム2から取得される。

【0029】9は署名付き電子情報i 6 aより取り出した電子情報i 1 bとユーザ署名i 2 bとを受け取りユーザ公開鍵P uを用いてユーザ署名i 2 bの正当性を検証するユーザ署名検証手段である。ここで、ユーザ署名i 2 b、電子情報i 1 bは、更新対象となる署名付き電子情報i 6 bに含まれる情報であり、それぞれ図2に示したユーザ署名i 2 a、電子情報i 1 aに相当する。すなわち、ユーザ署名i 2 aとユーザ署名i 2 b、電子情報i 1 aと電子情報i 1 bは、署名付き電子情報i 6 aが不正に書き換えられていない限り、同一のものである。また、ユーザ公開鍵P uは、ユーザ秘密鍵S uに対応する復号のための鍵であり、ユーザ側システム1に記憶さ

れている。

【0030】次に、動作について説明する。センタ側システム2に記憶された有効期限i 4の期限切れが近づくと、署名付き電子情報i 6 aを更新しなければならない。そこで、まずセンタ側システム2の有効期限保管手段7は、複数のセンタ署名i 5 aの有効期限i 4を監視する。そして、有効期限i 4が近づいたセンタ署名i 5 aを発見すると、当該センタ署名i 5 aに対応する署名付き電子情報i 6 aを管理するユーザ側システム1に対して期限切れ警告i 7を送信する。この期限切れ警告i 7は対象となるセンタ署名i 5 aを指定して行われる。この期限切れ警告i 7を行うことによって、ユーザー側システム1の署名付き電子情報の署名更新し忘れを防止することができる。

【0031】この期限切れ警告i 7はユーザ側システム1によって受信され、署名付き電子情報i 6 aが不正に改変されていないかが検証される。この検証は、ユーザ署名i 2 b及びセンタ署名i 5 bの両面から行われるため、ユーザ側システム1単独、若しくはセンタ側システム2単独では、改変できないような厳重な鍵を掛けることができる。まず、ユーザ側システム1が期限切れ警告i 7を受け付けると、ユーザ署名手段4が署名付き電子情報i 6 bから電子情報i 1 bを取得し、図2を用いて説明したと同様にユーザ署名i 2 aを生成する。次に、MD生成手段5はユーザ署名i 2 aを受け取り、再生成MD i 8を生成する。この再生成MD i 8は図2を用いたMD i 3の生成方法と同様の方法で行われ、電子情報i 6 bが不正に改変されていない場合には、図2のMD i 3と同一の情報となる。

【0032】つぎに、センタ署名検証手段8 aが再生成MD i 8、センタ署名i 5 b、及び有効期限i 4 bを受け取り、センタ公開鍵P cによるセンタ署名の検証を行う。この検証はセンタ署名i 5 b、再生成MD i 8、有効期限i 4 b、及びセンタ秘密鍵S cに対応するセンタ公開鍵P cを用いて、周知の技術である署名検証処理によって実行される。この署名検証処理の一例としては、RSA暗号系の署名検証処理を用いることができる。また、他のデジタル署名に用いられる暗号系の署名検証処理を用いてもよい。他の暗号系及び検証結果が得られる関数については、「電子情報通信ハンドブック」p361、電子情報通信学会編、オーム社(1988)に記載されている。

【0033】上述の検証からセンタ署名i 5 bが正当であるか否かを示すセンタ署名検証結果i 9 aが生成される。センタ署名i 5 bがセンタ側システム2で作られたものであり、かつ電子情報i 1 b及び有効期限i 4 bが不正に書き換えられていない場合にはセンタ署名検証結果i 9 aは「正当」という値で出力される。それ以外のセンタ署名i 5 bがセンタ側システム2で作られたものでない場合には、又は、電子情報i 1 b若しくは有効期

11

限 i 4 b が不正に書き換えられている場合には、センタ署名検証結果 i 9 a は「不正」という値で出力される。なお、ここで有効期限 i 4 を過ぎていないかを検証してもよい。有効期限 i 4 を過ぎている場合にはセンタ署名検証結果 i 9 a は「不正」という値で出力する。

【0034】次に、ユーザ署名の検証について説明する。期限切れ警告 i 7 を受け付けたとき、ユーザ署名検証手段 9 がユーザ署名の正当性を検証する。まず、署名付き電子情報 i 6 a から電子情報 i 1 b とユーザ署名 i 2 b を取り出す。そして、電子情報 i 1 b、ユーザ署名 i 2 b、及びユーザ秘密鍵 S u に対応するユーザ公開鍵 P u を用いてユーザ署名検証処理を行い、ユーザ署名検証結果 i 10 a を生成する。このユーザ署名検証処理は、上述のセンタ署名検証処理と同様の方法で行うことができる。以上の処理により、センタ署名 i 5 b とユーザ署名 i 2 b の検証結果が得られる。

【0035】次に、図 4 を用いて署名付き電子情報 i 6 a の更新処理動作を説明する。図 4 は更新処理動作を説明する機能ブロック図であり、図 1、図 2 又は図 3 は同一の符号は同一又は相当の部分を表している。10 はセンタ署名検証結果 i 9 a とユーザ署名検証結果 i 10 a とを受け付け、センタ署名検証結果 i 9 a とユーザ署名検証結果 i 10 a とが共に「正当」を示した場合に、署名付き電子情報 i 6 a が改変されていない正当なものであると判断し、この判断結果に基づいて MD 生成手段 5 を制御して新 MD i 3 b を出力させる更新制御手段である。

【0036】更新処理動作は以下のように行われる。まず、更新制御手段 10 によりセンタ署名検証結果 i 9 a とユーザ署名検証結果 i 10 a とが共に「正当」を示しているかを判断する。共に「正当」を示している場合には、MD 生成を指示する制御信号を MD 生成手段 5 へ出力する。検証結果のどちらか一方、又は、両方が「不正」を示している場合には、署名付き電子情報 i 6 a、センタ署名 i 5 b、ユーザ署名 i 2 b が改変された、或いは、署名者が不当であると判断して、エラーを出力し、署名付き電子情報 i 6 a の更新を中止する。

【0037】更新制御手段 10 から MD 生成を指示する制御信号を受け付けた MD 生成手段は、図 2 にて説明した MD i 3 の生成と同様に MD i 3 を生成し、新 MD i 3 b としてセンタ側システム 2 へ送信する。この際、新 MD i 3 b の生成に用いるユーザ署名は、署名付き電子情報 i 6 a から取得する。また、新 MD i 3 b と合わせてセンタ署名 i 5 b も送信する。図 4 では、センタ署名 i 5 b を MD 生成手段 5 より新 MD i 3 b と一緒に送信しているが、新 MD i 3 b と一緒にセンタ署名 i 5 b を送信し、或いは MD 生成手段 5 を経由して送信する必要は必ずしもなく、結果として更新時にセンタ署名 i 5 b と新 MD i 3 b がセンタ側システム 2 に送信されればよい。例えば、センタ署名 i 5 b の送信は、署名付き電子

10

20

30

40

50

12

情報 i 6 a の正当性を確認した MD 更新制御手段 10 が行ってもよいし、別個に設けられた送信手段によって行っててもよい。

【0038】次に、センタ署名 i 5 b 及び新 MD i 3 b を受け取ったセンタ側システム 2 は、センタ署名 i 5 b の更新を開始する。まず、センタ署名検証手段 8 b はセンタ署名 i 5 b の正当性を検証し、その検証結果をセンタ署名検証結果 i 9 b として出力する。センタ署名 i 5 b の正当性の判断は、ユーザ側システム 1 のセンタ署名検証手段 8 a と同様の処理で行うことができる。また、そのセンタ署名検証結果 i 9 b は、「正当」又は「不正」のいずれかである。

【0039】また、センタ署名 i 5 a の生成時に有効期限 i 4 及び MD i 3 について署名した場合においては、有効期限 i 4 をもセンタ署名の検証処理に用いる。この有効期限 i 4 は、有効期限保管手段 7 から取得された新 MD i 3 b に対応する有効期限 i 4 である。このとき、この有効期限 i 4 と現在の日時とを比較して、有効期限 i 4 を過ぎていないかを判断する。有効期限 i 4 を過ぎている場合にも、センタ署名検証結果 i 9 a は「不正」という値で出力される。一方、センタ署名検証結果 i 9 a 「正当」という値で出力される場合は、第 1 にセンタ署名 i 5 b がセンタ側システム 2 で作られた正当なものであること、第 2 に有効期限 i 4 を過ぎていないこと、の 2 つの要件全てを備える場合である。有効期限 i 4 が過ぎると、センタ署名 i 5 b を解読される可能性が高くなるが、この有効期限 i 4 の検査処理を行うことにより、署名付き電子情報 i 6 a が有効期限 i 4 内で更新されたことが確認でき、署名付き電子情報 i 6 a の信頼性がより高くなる。

【0040】センタ署名手段 6 は、センタ署名検証結果 i 9 b が「正当」である場合、新たにセンタ秘密鍵 P c を生成し、このセンタ秘密鍵 S c を新センタ秘密鍵 new S c とし、さらに、この新センタ秘密鍵 new S c を用いて新センタ署名 i 5 c を生成する。新センタ署名 i 5 c は図 2 を用いて説明したセンタ署名 i 5 a と同様に行われる。このとき、新 MD i 3 b は MD i 3 、新センタ秘密鍵 new S c はセンタ秘密鍵 S c に相当する。また、図 2 を用いて説明した署名付き電子情報の作成処理と同様に、新たな有効期限 i 4 を設定し、この有効期限 i 4 をも含めて新センタ署名 i 5 c を生成する。新たに設定された有効期限 i 4 と生成された新センタ署名 i 5 c は、ステップ S 5 としてセンタ署名手段 6 よりユーザ側システム 1 へ送信される。

【0041】新センタ署名 i 5 c と有効期限 i 4 を受信したユーザ側システム 1 は、図 2 を用いて説明した署名付き電子情報の作成と同様に作成処理を行い、新しい署名付き電子情報 i 6 b を生成する。このとき、新しい署名付き電子情報 i 1 b は電子情報 i 1 b 、ユーザ署名 i 2 b 、有効期限 i 4 及び新センタ署名 i 5 c により生成

される。生成された署名付き電子情報 i 1 b はユーザ側システム 1 に記憶される。以上で、署名付き電子情報 i 6 a の更新が終了する。なお、この署名の更新は何度も繰り返すことができる。

【0042】この実施の形態 1 では、署名付き電子情報に有効期限を含ませたが、必要に応じて、有効期限を含ませないようにすることもできる。

【0043】以上の電子情報署名システムによれば、更新時に署名付き電子情報の検証を行っているため、更新前の署名付き電子情報 i 6 a における電子情報 i 1 a と更新後の署名付き電子情報における電子情報 i 1 b とが同一のものであることが保証され、かつ、有効期限 i 4 内に解読されないような大きさの比較的小さいサイズの署名を付加すればよいため、署名付き電子情報のデータサイズを小さくすることができます。そして、更新を繰り返せば、署名の大きさに関わらず長期間に渡って文書の安全性、すなわち不正な改変、偽造等がないこと、が高い信頼性をもって保証できる。

【0044】実施の形態 2、実施の形態 2 は、センタ側システムでセンタ署名を自動的に更新し、電子情報の安全性を確保しつつ、ユーザ側システムとセンタ側システムの通信量を減少させる実施の形態である。

【0045】図 5 はこの実施の形態 2 の電子情報署名システムのデータの流れを説明するシーケンス図であり、署名付き電子情報の作成、更新処理、に加えて検証処理についてもその処理シーケンスを示している。図 5において、図 1 と同一の符号は同一又は相当の部分を表す。1 2 は署名付き電子情報の持つ有効期限の期限切れが近づくと、センタ側システム 2 に記憶した MD i 3 若しくはセンタ署名 i 5 c 等の電子情報に関する情報を新しいセンタ秘密鍵 n e w S c を用いて暗号化し、新センタ署名を生成する電子センタ署名更新手段である。この新センタ署名にも、有効期限 i 4 が設定されており、新たに設定した有効期限 i 4 の期限切れが近づくと、再びセンタ署名の更新が行われる。

【0046】次に動作について概要を説明する。署名付き電子情報の作成は、まず、ステップ S 1 で、実施の形態 1 と同様に MD i 3 が生成され、センタ側システム 2 側に送信され、センタ側システム 2 によって MD i 3 からセンタ署名 i 5 a が生成される。次に、ステップ S 2 に移り、生成したセンタ署名 i 5 a に識別子を付してセンタ側システム 2 で記憶するとともに、付した識別子をユーザ側システム 1 に送信する。識別子を受け取ったユーザ側システム 1 は、識別子と電子情報 i 2 a を組み合わせて署名付き電子情報 i 6 c として記憶する。

【0047】署名付き電子情報の作成が終了し、有効期限 i 4 の期限切れが近づくと、署名付き電子情報の更新が行われる。署名付き電子情報の更新は、実施の形態 1 と異なりセンタ側システム 2 側で行い、ユーザ側システム 1 との MD i 3 及びセンタ署名 i 5 a の交信は行わな

い。このため、ユーザ側システム 1 の処理負担を軽減すると共に、ユーザ側システム 1 及びセンタ側システム 2 を合わせたシステム全体としても通信量が削減されるので処理効率がよい。

【0048】センタ側システム 2 は複数のセンタ署名 i 5 a を管理する。ここで 1 つのセンタ署名 A の有効期限 i 4 の期限切れが近づいた場合の更新動作を説明すると、このセンタ署名 A について新たに新センタ秘密鍵 N e w S c と有効期限 i 4 とを設定し、この新センタ秘密鍵 N e w S c を用いて、自己のシステムに記憶した MD i 3、若しくはセンタ署名 i 5 a 等の電子情報に関する情報から新たにセンタ署名 i 5 a を生成する。そして、生成したセンタ署名 i 5 a をセンタ署名 A の識別子に対応するセンタ署名 i 5 a として記憶する。

【0049】以降、有効期限 i 4 の期限切れが近づく度に同様の処理を行い。次々とセンタ署名を更新する。そのため、センタ秘密鍵 S c を解読される危険性が極めて少なく、電子情報の不正な改変、偽造を防止することができる。また、更新時には実施の形態 1 と同様にセンタ署名の検証を行い、検証結果が「正当」である場合に更新を行うため、長期にわたって電子情報が改変されていないことが保証できる。

【0050】この電子情報署名システムでは、ユーザ側システム 1 はセンタ署名 i 5 a に対応する識別子を持っているだけなので、このままでは、センタ署名 i 5 a による電子情報の正当性を検証できない。そこで、次に、署名付き電子情報の検証処理について説明する。まず、ユーザ側システム 1 は、ステップ S 6 で、検証しようとする署名付き電子情報から新 MD i 3 b を生成し、この新 MD i 3 b を当該署名付き電子情報に対応する識別子とともに送信する。

【0051】センタ側システム 2 では、送信された新 MD i 3 b 及び識別子を受け取り、新 MD i 3 b が改変されていないかどうか、新 MD i 3 b と識別子に対応するセンタ署名とセンタ公開鍵 P c とを用いて検証する。このセンタ署名の検証は、実施の形態 1 で説明したのと同様に行われる。

【0052】そして、ステップ S 7 にて、検証結果をユーザ側システム 1 へ送信する。ユーザ側システム 1 では、受け取った検証結果及びユーザ側システム 1 が独自に実施するユーザ署名 i 2 a による検証結果に基づいて、署名付き電子情報の正当性を判断する。

【0053】以上の電子情報署名システムによれば、センタ署名の更新時に MD を送信しないため、更新が高速に行え、かつユーザ側システム 1 かかる処理負荷を軽減することができる。また、ユーザ側システム 1 とセンタ側システム 2 との間の回線に発生する障害によって、センタ署名 i 5 a の更新が行えず有効期限 i 4 を過ぎてしまうといった問題も生じない。

【0054】実施例 2-1

◇システム詳細

次に、図5に示した電子情報署名システムの署名付き電子情報の作成処理、更新処理、及び検証処理の詳細について、それぞれ図6、図7、及び図8を用いて説明する。特に、この実施例2-1では、センタ署名更新のためにMD i 3を保存し、このMD i 3に基づいて新センタ署名 i 5 dを生成する方法を用いている。図6は、この実施の形態2の電子情報署名システムの署名付き電子情報の作成処理を説明する機能ブロック図である。図6において、図5又は図2と同一の符号は同一又は相当の部分を表す。13はセンタ署名手段6が生成したセンタ署名 i 5 aを保管し、保管したセンタ署名 i 5 aの識別子 i 5 dを出力する署名保管手段、16はセンタ秘密鍵S cとこのセンタ秘密鍵S cに対応するセンタ公開鍵P cを生成するセンタ秘密鍵生成手段である。

【0055】・署名付き電子情報作成処理

次に署名付き電子情報 i 6 c の作成処理について説明する。まず、ユーザ側システム1の署名付き電子情報 i 6 c の作成処理は、基本的に実施の形態1と同様である。異なるのは、ステップS 2 bでセンタ側システム2より識別子 i 5 dを受け取り、センタ署名 i 5 aの代わりに受け取った識別子 i 5 dを署名付き電子情報 i 6 cとして保存する点である。従って、署名付き電子情報 i 6 c は、電子情報 i 1 a、ユーザ署名 i 2 a、及び識別子 i 5 dにより構成される。

【0056】次に、センタ側システム2での処理について説明すると、ステップS 1で送信されたMD i 3を受け取ったセンタ側システム2は、センタ秘密鍵S c、センタ公開鍵P c、及び有効期限 i 4を生成し、実施の形態1の図2で説明したのと同様にセンタ署名 i 5 aを生成する。このとき署名保管手段13は、このセンタ署名 i 5 aと、このセンタ署名 i 5 aに対応するセンタ公開鍵P c、有効期限 i 4及びMD i 3とを1つのセンタ署名情報 i 11として記憶する。この際、記憶したセンタ署名情報には他のセンタ署名情報の識別子とは異なる値を持つ識別子 i 5 dが割り当てられ、ステップS 2 bでユーザ側システム1に送信される。識別子 i 5 dには、例えば、署名保管手段13におけるセンタ署名情報のアドレスを用いることができる。アドレスを用いた場合には、識別子 i 5 dをキーとして高速にセンタ署名情報を検索できる。

【0057】識別子 i 5 dを受け取ったユーザ側システム1では、上述のように識別子 i 5 dを署名付き電子情報 i 6 cとして保存する。この署名付き電子情報 i 6 c は、実施の形態1のようにセンタ署名 i 5 aを直接保存する場合と比べて、データサイズが少なく記憶容量を節約することができるという特徴がある。すなわち、センタ署名 i 5 aは、MD i 3及び有効期限 i 4を暗号化した情報であるため、所定のデータサイズを有する。一方、識別子 i 5 dは数バイトのデータ量で構成できるた

め、データサイズが小さいという特徴がある。以上で署名付き電子情報 i 6 c の作成処理が完了する。

【0058】・署名付き電子情報更新処理

次に、署名付き電子情報の更新処理について、図7を用いて詳細に説明する。図7はこの実施の形態2の電子情報署名システムの署名付き電子情報の更新処理を説明する機能ブロック図である。図7において、図6と同一の符号は同一又は相当の部分を表す。

【0059】次に、動作について説明する。署名保管手段13は複数のセンタ署名情報 i 11 を記憶し、それらのセンタ署名情報 i 11 のうち有効期限 i 4 の期限切れが近づいているものがないかを常時監視している。もし、期限切れが近づいているものを発見した場合には、センタ署名 i 5 aの更新処理を開始する。ここでは、複数のセンタ署名 i 5 aのうちの1つセンタ署名 Aについて更新処理を行う場合について説明する。まず、期限切れが近づいているセンタ署名 Aを発見すると、そのセンタ署名 Aに対応するMD i 3をセンタ署名手段6へ出力する。センタ署名手段6では、このMD i 3を受け取るとともに、センタ秘密鍵生成手段16に新たなセンタ秘密鍵S cとこのセンタ秘密鍵S cに対応するセンタ公開鍵P cとを生成させ、これらをそれぞれ新センタ秘密鍵New S c、新センタ公開鍵new P cとして受け取る。さらに、図示しない有効期限設定手段に新たな有効期限 i 4を設定させる。そして、受け取ったMD i 3と新しい有効期限 i 4を新センタ秘密鍵New S cを用いて署名し、新センタ署名 i 5 aを生成する。

【0060】この新センタ署名 i 5 aは署名保管手段13へ出力され、署名保管手段13は受け取った新センタ署名 i 5 aを新たに設定された有効期限 i 4、センタ公開鍵new P cとともに記憶する。図9は、署名保管手段13内の記憶内容を示すメモリマップの例である。センタ署名 i 5 aが更新される前は、1つの識別子 i 5 dに対するセンタ署名情報 i 11 として、MD i 3、有効期限A、センタ公開鍵P c A、センタ署名A、有効期限B、センタ公開鍵P c B、及びセンタ署名Bを記憶している。有効期限A及び有効期限Bは、それぞれセンタ署名A、Bに対する有効期限 i 4であり、センタ署名Aは最初に記憶されたセンタ署名 i 5 a、センタ署名Bは2番目に記憶されたセンタ署名 i 5 aである。また、各センタ公開鍵P c A、Bは、それぞれセンタ署名A、Bに対応するセンタ公開鍵P c である。

【0061】センタ署名が更新されると、MD i 3、有効期限A、センタ公開鍵P c A、センタ署名A、有効期限B、センタ公開鍵P c B、及びセンタ署名Bに加えて、新センタ署名 i 5 dであるセンタ署名C、このセンタ署名Cに対する新しい有効期限C、及び新センタ公開鍵new P cがセンタ公開鍵P c Cとして図9のように記憶される。

【0062】ここでは、過去にセンタ署名 i 5 aが正常

17

に更新されたかを検証できるようにするため、過去のセンタ署名 i 5 a の履歴を記憶しているが、古くなったセンタ署名 i 5 a 、有効期限 i 4 、及びセンタ公開鍵 P c は消去しても良い。この場合には、多数の更新が行われても署名保管手段 1 3 の必要記憶容量が変化しないという利点がある。

【0063】・署名付き電子情報検証処理

次に、署名付き電子情報の検証処理について、図 8 を用いて詳細に説明する。図 8 はこの実施の形態 2 の電子情報署名システムの署名付き電子情報の検証処理を説明する機能ブロック図である。図 8において、図 6 と同一の符号は同一又は相当の部分を表す。1 4 は識別子 i 5 d に基づき署名保管手段 1 3 よりセンタ署名情報 1 1 を検索するセンタ署名検索手段、1 5 はユーザ署名検証手段 9 よりユーザ署名検証結果 i 10 a を、センタ署名検証手段 1 7 a よりセンタ署名検証結果 i 9 b を受け取り、これらの検証結果に基づいて署名付き電子情報 i 6 c を検証する電子情報検証手段である。1 7 a はセンタ署名情報 i 1 1 及び再生 MD i 8 を受け取り、センタ署名 i 5 d を検証するセンタ署名検証手段 1 7 a である。

【0064】次に、動作について説明する。署名付き電子情報 i 6 c を検証する場合には、まず、ユーザ署名手段 4 が電子情報 i 1 b からユーザ秘密鍵 S u を用いてユーザ署名を生成する。そして、MD生成手段 5 がユーザ署名から MD i 3 を生成し、ステップ S 6 で、この MD i 3 を再生成 MD i 8 として送信する。このとき、再生性 MD i 8 に対応する当該署名付き電子情報 i 6 c の識別子 i 5 d も送信される。この送信は、センタ署名 i 5 a を用いた検証のために行われる。一方、ユーザ側システム 1 でもユーザ署名 i 2 b を用いた検証が行われる。この検証は、図 3 を用いて説明した通りである。

【0065】ステップ S 6 で送信された再生成 MD i 8 及び識別子 i 5 d を受信したセンタ側システム 2 では、センタ署名 i 5 a を用いた検証が行われる。まず、識別子 i 5 d を受け取ったセンタ署名検索手段 1 4 は、識別子 i 5 d をキーとして、署名保管手段 1 3 に記憶された複数のセンタ署名情報 i 1 1 の中から、当該識別子 i 5 d に対応するセンタ署名情報 i 1 1 を検索する。検索されたセンタ署名情報 i 1 1 はセンタ署名検証手段 1 7 a へ出力される。

【0066】センタ署名検証手段 1 7 a は、ユーザ側システム 1 から受け取った再生成 MD i 8 、センタ署名検証手段 1 4 から受け取ったセンタ署名情報 i 1 1 を用いてセンタ署名を検証する。すなわち、この検証は、センタ署名情報 1 1 に含まれる最新（現在）の有効期限 i 4 及びセンタ公開鍵 P c と、ユーザ側システム 1 から受け取った再生成 MD i 8 とを用い実施の形態 1 で説明したセンタ署名の検証処理と同様に行われる。検証の結果は、ステップ S 7 でセンタ署名検証結果 i 9 b として出力される。

18

【0067】なお、ここでセンタ署名が期限内に正常に更新されていたかを検証してもよい。この場合は、センタ署名情報 i 1 1 に記憶されている過去のセンタ署名の履歴（センタ署名、有効期限、センタ公開鍵）を用いて上述のように検証をする。例えば、図 9 の更新後の例では、有効期限 B 、センタ公開鍵 P c B 、及びセンタ署名 B を用いて上述のセンタ署名検証処理を行えば前回の更新が正当にかつ有効期限内に行われたかを検証することができる。さらに、有効期限 A 、センタ公開鍵 P c A 、及びセンタ署名 A を用いて上述のセンタ署名検証処理を行えば、3 回前の更新が正当に行われたかを検証することができる。このような過去の更新履歴まで検証する場合には、全ての検証結果が「正当」を示したときに、センタ署名検証結果 i 9 b を「正当」とする。過去の履歴において、「不正」が検出された場合には、そのときにセンタ署名が解読されていないことを保証できないため、センタ署名検証結果 i 9 b を「不正」とする。過去の更新履歴まで検証する場合の効果は、過去においてセンタ署名が正常に更新されていたことが保証されるため、より厳密な検証を行えるということにある。

【0068】ステップ S 7 にて、上述のようにセンタ署名検証結果 i 9 b が送信されるとユーザ側システム 1 で最終的な署名付き電子情報 i 6 c の検証処理が行われる。センタ側システム 2 から送信されたセンタ署名検証結果 i 9 b は、電子情報検証手段 1 5 に受け取られる。電子情報検証手段 1 5 では、ユーザ署名検証結果 i 10 a とセンタ署名検証結果 i 9 b に基づいて、署名付き電子情報の検証結果、すなわち、電子情報検証結果 i 12 を出力する。このとき、電子情報検証結果 i 12 が「正当」を示す場合は、ユーザ署名検証結果 i 10 a 及びセンタ署名検証結果 i 9 b がともに「正当」である場合であり、それ以外は、「不正」を出力する。

【0069】以上のように、この実施例によれば、センタ署名の更新時に MD を送信しないため、更新が高速に行え、かつユーザ側システム 1 かかる負荷を軽減することができる。また、ユーザ側システム 1 とセンタ側システム 2 との間の回線に発生する障害によって、センタ署名 i 5 a の更新が行えず有効期限 i 4 を過ぎてしまうといった問題も生じない。

【0070】実施例 2-2 次に、図 5 に示した電子情報署名システムの署名付き電子情報の更新処理、及び検証処理の詳細について他の実施例を図 10 及び図 11 を用いて説明する。特に、この実施例 2-2 では、実施の形態 2-1 と異なり、センタ署名を新しいセンタ秘密鍵にて繰り返し暗号化する方法を用いて、センタ署名の解読を防止している。図 10 は、この実施例 2-2 の電子情報署名システムの署名付き電子情報の更新処理を説明する機能ブロック図である。図 10 において、図 5 又は図 7 と同一の符号は同一又は相当の部分を表す。

【0071】次に動作について説明する。署名付き電子

19

情報の作成処理については、基本的に同様の処理が行われるため説明を省略する。ただし、後述するように署名保管手段13に記憶される情報を変更しても良い。例えば、MDi3を記憶する必要は必ずしもないので、MDi3を記憶しないこととしてもよい。

【0072】・署名付き電子情報更新処理

続いて、図10を用いて、署名付き電子情報の更新処理について説明する。まず、有効期限i4の期限切れが近づくと、署名保管手段7がセンタ署名手段6へセンタ署名i5eを出力する。このセンタ署名i5eは、現在有効な更新前のセンタ署名i5aである。また、このとき新たに有効期限i4が設定され、さらにセンタ秘密鍵生成手段16が新センタ秘密鍵newSc及びこの新センタ秘密鍵newScに対応した新センタ公開鍵newPcを生成する。

【0073】センタ署名手段6は、センタ署名i5e、新センタ秘密鍵newSc、及び有効期限i4を受け取り、新センタ秘密鍵newScを用いてセンタ署名i5e及び有効期限i4を暗号化し、新センタ署名i5fを生成する。

【0074】センタ署名手段6が生成した新センタ署名i5fは、署名保管手段7へ出力される。署名保管手段7は、新センタ公開鍵newPc、及び有効期限i4とともにこの新センタ署名i5fを新たに追加記憶する。この際、更新前のセンタ署名i5e、更新前の有効期限i4、及び更新前のセンタ公開鍵Pcは消去せずに記憶しておく。例えば、図9に示すように記憶され、更新される。ただし、この実施例においては、センタ署名情報i11にMDを記憶しておく必要はない。以上の更新処理が有効期限i4が近づく度に実行される。

【0075】・署名付き電子情報検証処理

次に、署名付き電子情報検証処理について説明する。署名付き電子情報の検証処理は、図8を用いて実施の形態2-1で説明したものと同様に行われる。ただし、センタ署名検証手段17aで行われる検証処理がことなるため、ここではその検証処理について図11を用いて説明する。

【0076】*センタ署名検証手段の検証処理

図9に示した更新後のセンタ署名情報i11を例にとって、以下にその検証処理を説明する。まず、最初にステップS20～S22で現在のセンタ署名及び過去のセンタ署名i5e、fについて、検証処理を行う。ステップS20～S22の処理は、入れ替え可能でどのような順番で実行してもよい。例えば、ステップS22→S20→S21の順番で実行してもよい。以下にそれぞれの処理について説明する。

【0077】ステップS20では、ユーザ側システム1から受け取った再生成MDi8を最初に設定されたセンタ署名Aで検証する。この検証処理は、再生成MDi8、有効期限A、センタ公開鍵PcA、及びセンタ署名

50

20

Aを用いて、実施の形態1で説明したセンタ署名の検証処理と同様に行われ、その検証結果（すなわち、署名A検証結果i20）が「正当」又は「不正」のいずれかで出力される。例えば、センタ署名Aをしたときの電子情報i1aと検証時の電子情報i1bとが異なる場合、署名A検証結果i20は「不正」という値で出力され、ユーザ側システム1に記憶されている電子情報i1bの正当性を検証することができる。

【0078】ステップS21では、センタ署名A、有効期限B、センタ署名B、及びセンタ公開鍵PcBを用いてセンタ署名A、及び有効期限Bが不正に書き換えられていなかどうか正当性を検証する。この検証処理は、ステップS20と同様に行い、署名B検証結果i21を得る。

【0079】ステップS22では、センタ署名B、有効期限C、センタ署名C、及びセンタ公開鍵PcCを用いてセンタ署名B、及び有効期限Cが不正に書き換えられていなかどうか正当性を検証する。この検証処理は、ステップS20と同様に行い、署名C検証結果i22を得る。

【0080】以上の処理では、2回の更新が行われた場合の検証処理を説明したが、n回の更新が行われた場合には、それぞれの更新時に生成したセンタ署名を用いて、前回のセンタ署名i5e及び有効期限i4の正当性をステップS21又はS22と同様に検証する。

【0081】次にステップS23に移り、最後に、全ての署名検証結果（すなわち、署名A検証結果i20、署名B検証結果i21、署名C検証結果i22）に基づいてセンタ署名検証結果i9bを出力する。ここでは、全ての署名検証結果が「正当」を示しているかを判断する。すべて、「正当」を示している場合は、センタ署名検証結果i9bとして「正当」を出力する。それ以外場合は、「不正」を出力する。

【0082】以上により得られたセンタ署名検証結果i9bは、ユーザ側システム1へ送信され、実施例2-1で説明したように電子情報検証結果i11が求められる。

【0083】以上、この実施例によれば、センタ署名を有効期限i4毎に異なる暗号で次々と暗号化し、署名の更新を行うため、長期にわたって署名付き電子情報i6aが改変されていないことが保証できる。さらに、署名の更新はセンタ側システム2内で行うため、ユーザ側システム1側の負荷が少ないという利点がある。また、更新前のセンタ署名を記憶せず、更新後のセンタ署名から生成するため、記憶容量を節約できるという利点がある。

【0084】

【発明の効果】この発明は、以上に説明したように構成されているので、以下に記載されるような効果を奏する。

21

【0085】この発明にかかる電子署名方法においては、第1のシステムが、第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、第2のシステムが、受信した第1の情報を第1の秘密鍵を用いて電子署名することにより生成した第1の署名情報を第1のシステムへ送信する第2の送信ステップと、第1のシステムが、第1の署名情報を記憶する第1の記憶ステップと、第1の署名情報の有効期限に基づいた更新時期に第1のシステムが、第1の記憶ステップで記憶された第1の署名情報を用いて電子情報が正当であるか否かを検証する検証ステップと、この検証ステップの検証結果が正当であると判断された場合に第1のシステムが、第1の情報を第2のシステムへ送信する第3の送信ステップと、第2のシステムが、第3の送信ステップで送信された第1の情報を第2の秘密鍵を用いて署名することにより生成された第2の署名情報を第1のシステムへ送信する第4の送信ステップと、第1のシステムが、第2の署名情報を記憶する第2の記憶ステップと、を備えたため、少ない署名情報で長期間にわたって電子情報の安全性を保つことができる。

【0086】また、第1の情報は、電子情報を第3の秘密鍵を用いて署名することにより生成した第3の署名情報に基づいて生成され、検証ステップは、第1の署名情報又は第3の署名情報の有効期限に基づいた更新時期に第1のシステムが、第1の署名情報及び第3の署名情報を用いて電子情報が正当であるか否かを検証するため、第1のシステム、第2のシステムの両方で電子署名が行われるため、一方のシステム単独で電子情報及び1つの署名情報を改変した場合でも、他の署名情報を新たに生成できないため、その改変を検出することができ、長期間にわたって電子情報の安全性をより高く保つことができる。

【0087】また、第1のシステムが、第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、第2のシステムが、受信した第1の情報を第1の秘密鍵を用いて電子署名することにより生成した第1の署名情報を第1のシステムへ送信する第2の送信ステップと、第1のシステムが、第1の署名情報を記憶する記憶ステップと、第1の署名情報の有効期限に基づいた更新時期に第1のシステムが、第1の情報を第2のシステムへ送信する第3の送信ステップと、第2のシステムが、第1の署名情報を用いて第1の情報が正当であるか否かを検証する検証ステップと、第1の検証ステップの検証結果が正当であると判断された場合に第2のシステムが、第1の情報を第2の秘密鍵を用いて署名することにより生成された第2の署名情報を送信する第4の送信ステップと、第1のシステムが、第2の署名情報を記憶する第2の記憶ステップと、を備えたため、長期間にわたって電子情報の安

10

20

30

40

50

22

全性を保つことができる。

【0088】また、電子情報を第3の秘密鍵を用いて署名することにより生成した第3の署名情報又は第1の署名情報の有効期限に基づいた更新時期に第1のシステムが、第3の署名情報を用いて電子情報が正当であるか否かを検証する第2の検証ステップを備え、第1の情報は、第3の署名情報に基づいて生成され、第3の送信ステップは、第2の検証ステップの検証結果が正当であると判断された場合に第1のシステムが、第1の情報を代えて、電子情報を第4の秘密鍵を用いて電子署名することにより生成した第4の署名情報に基づいて生成した第2の情報を第2のシステムへ送信し、第1の検証ステップは、第2のシステムが、第1の署名情報を用いて電子情報が正当であるか否かを検証し、第4の送信ステップは、第1の検証ステップの検証結果が正当であると判断された場合に第2のシステムが、第1の情報を代えて第2の秘密鍵を用いて電子署名することにより生成された第2の署名情報を送信するので、第1のシステム、第2のシステムの両方で電子署名が行われるため、一方のシステム単独で電子情報及び1つの署名情報を改変した場合でも、他の署名情報を新たに生成できないため、その改変を検出することができ、長期間にわたって電子情報の安全性をより高く保つことができる。

【0089】また、第1のシステムが、第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、第2のシステムが、受信した第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、第1の情報と第1の署名情報を第2のシステムに記憶する第1の記憶ステップと、第1の署名情報の有効期限に基づいた更新時期に第2のシステムが、第1の情報を第2の秘密鍵で電子署名することにより第2の署名情報を生成する第2の生成ステップと、第2の署名情報を記憶する第2の記憶ステップと、を備えたため、長期間にわたって電子情報の安全性を保つことができる。

【0090】また、第1のシステムが、第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、第2のシステムが、受信した第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、第1の情報と第1の署名情報を第2のシステムに記憶する第1の記憶ステップと、第1の署名情報の有効期限に基づいた更新時期に第2のシステムが、第1の署名情報を第2の秘密鍵を用いて電子署名することにより第2の署名情報を生成する第2の生成ステップと、第2の署名情報を第2のシステムに記憶する第2の記憶ステップと、を備えたため、長期間にわたって電子情報の安全性を保つことができる。

【図面の簡単な説明】

【図1】 この発明の実施の形態1における電子情報署名システムの署名／更新処理を説明するシーケンス図である。

【図2】 この発明の実施の形態1における電子署名システムの署名処理を説明する機能ブロック図である。

【図3】 この発明の実施の形態1における電子署名システムの検証／更新処理を説明する機能ブロック図である。

【図4】 この発明の実施の形態1における電子署名システムの署名更新処理を説明する機能ブロック図である。
10

【図5】 この発明の実施の形態2における電子情報署名システムの署名／更新／検証処理を説明するシーケンス図である。

【図6】 この発明の実施例2-1における電子署名システムの署名処理を説明する機能ブロック図である。

【図7】 この発明の実施例2-1における電子署名システムの更新処理を説明する機能ブロック図である。

【図8】 この発明の実施例2-1における電子署名シ

ステムの検証処理を説明する機能ブロック図である。

【図9】 この発明の実施例2-1におけるセンタ署名保管手段の記憶内容を示すメモリマップである。

【図10】 この発明の実施例2-2における電子情報署名システムの署名更新処理を説明する機能ブロック図である。

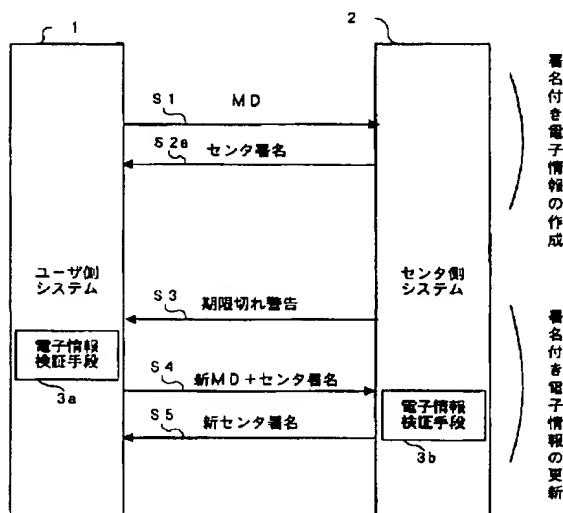
【図11】 この発明の実施例2-2における電子署名システムの検証処理を説明するフローチャートである。

【図12】 従来の電子情報署名装置の構成を説明する機能ブロック図である。

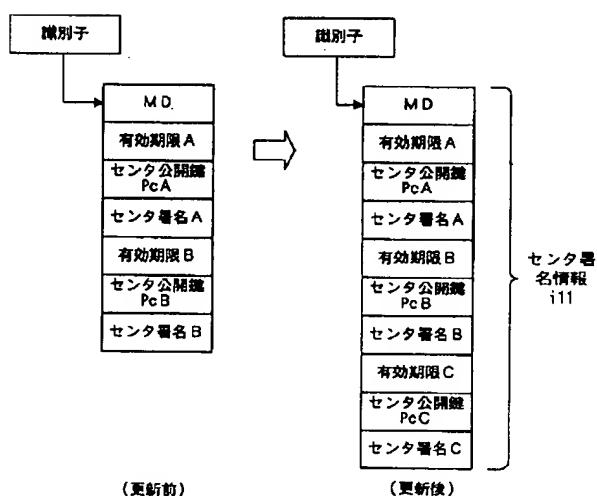
【符号の説明】

- 1 ユーザ側システム、 2 センタ側システム、 3 a, b 電子情報検証手段、 4 ユーザ署名手段、
5 MD生成手段、 6 センタ署名手段、 7 有効期限保管手段、 8 a センタ署名検証手段、 9 ユーザ署名検証手段、 10 更新制御手段、 11 署名付き電子情報生成手段、 12 センタ署名更新手段、
13 署名保管手段、 16 センタ秘密鍵生成手段、 17 センタ署名検証手段

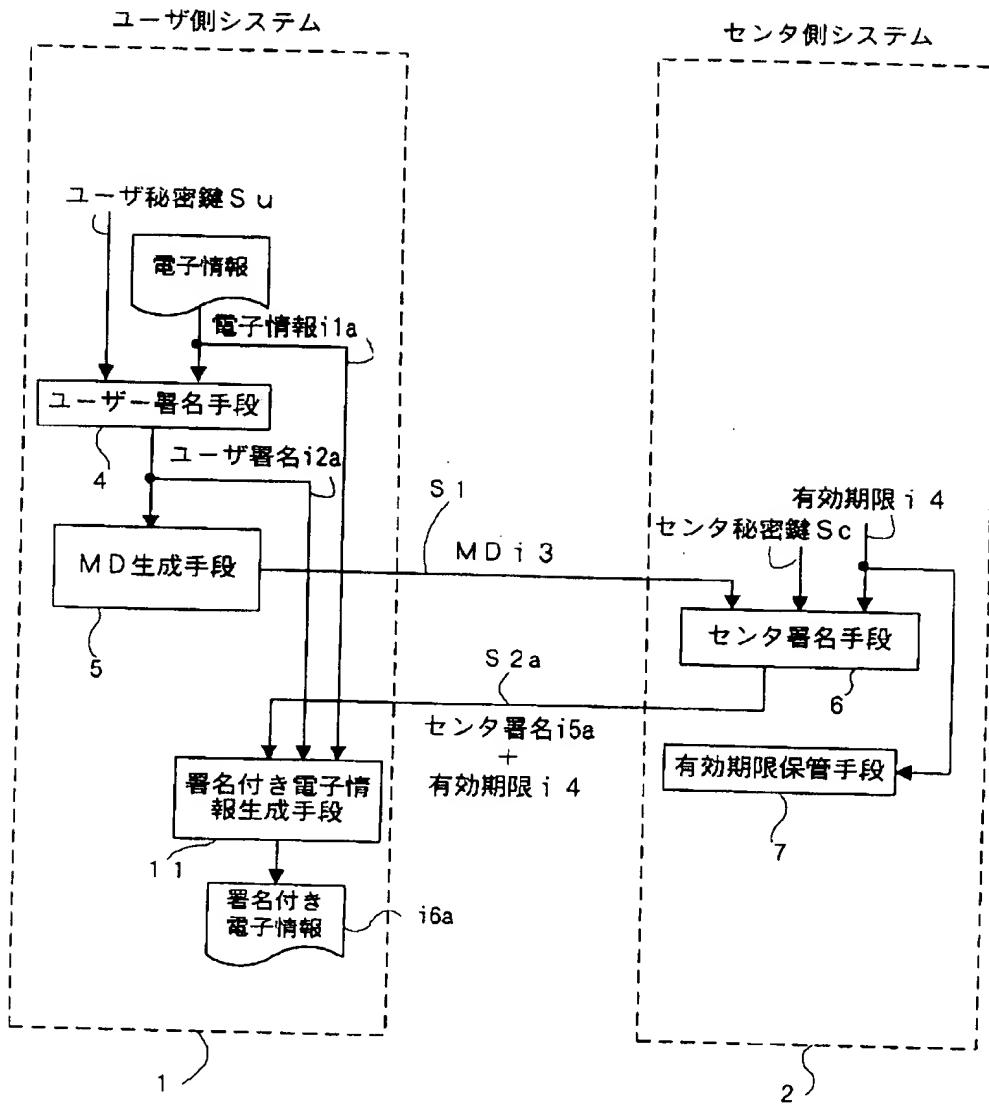
【図1】



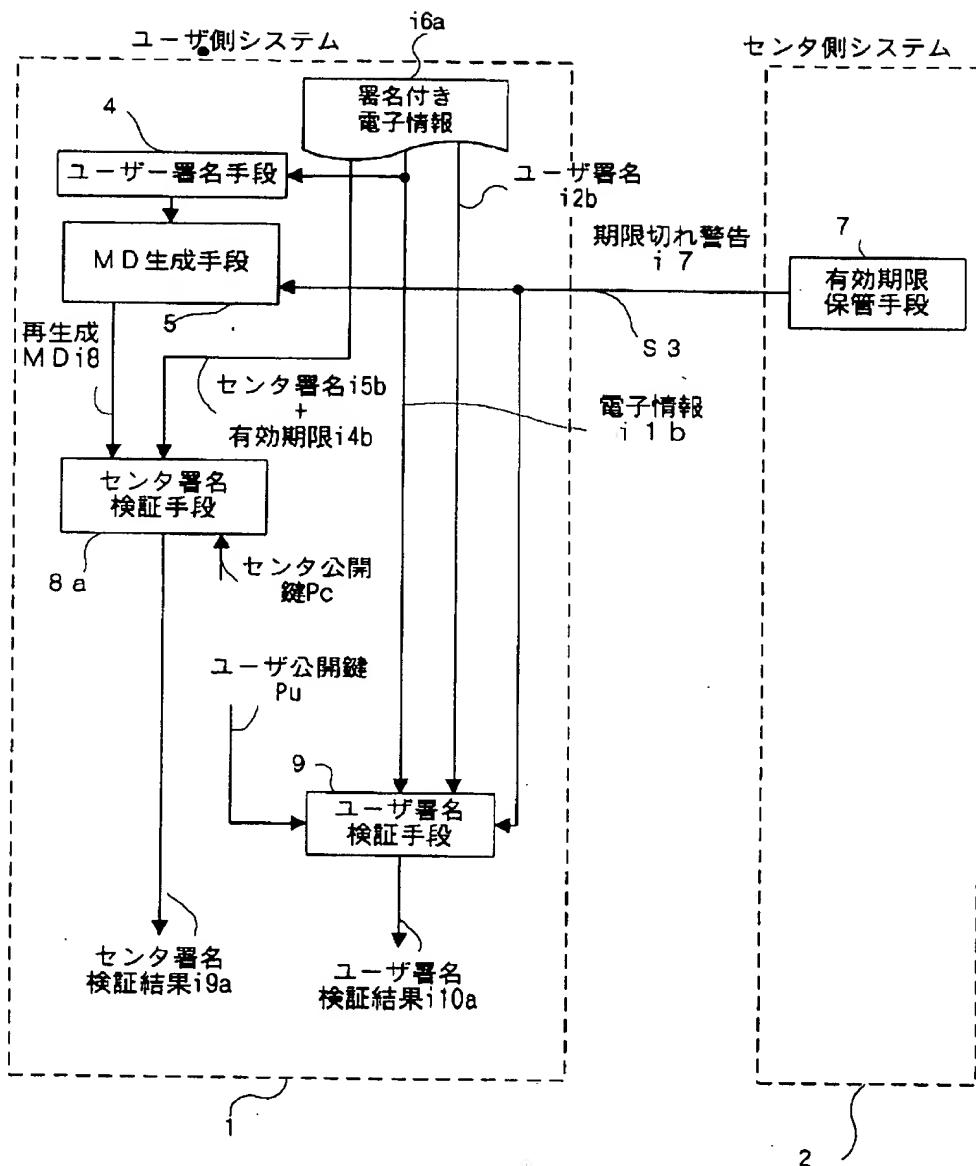
【図9】



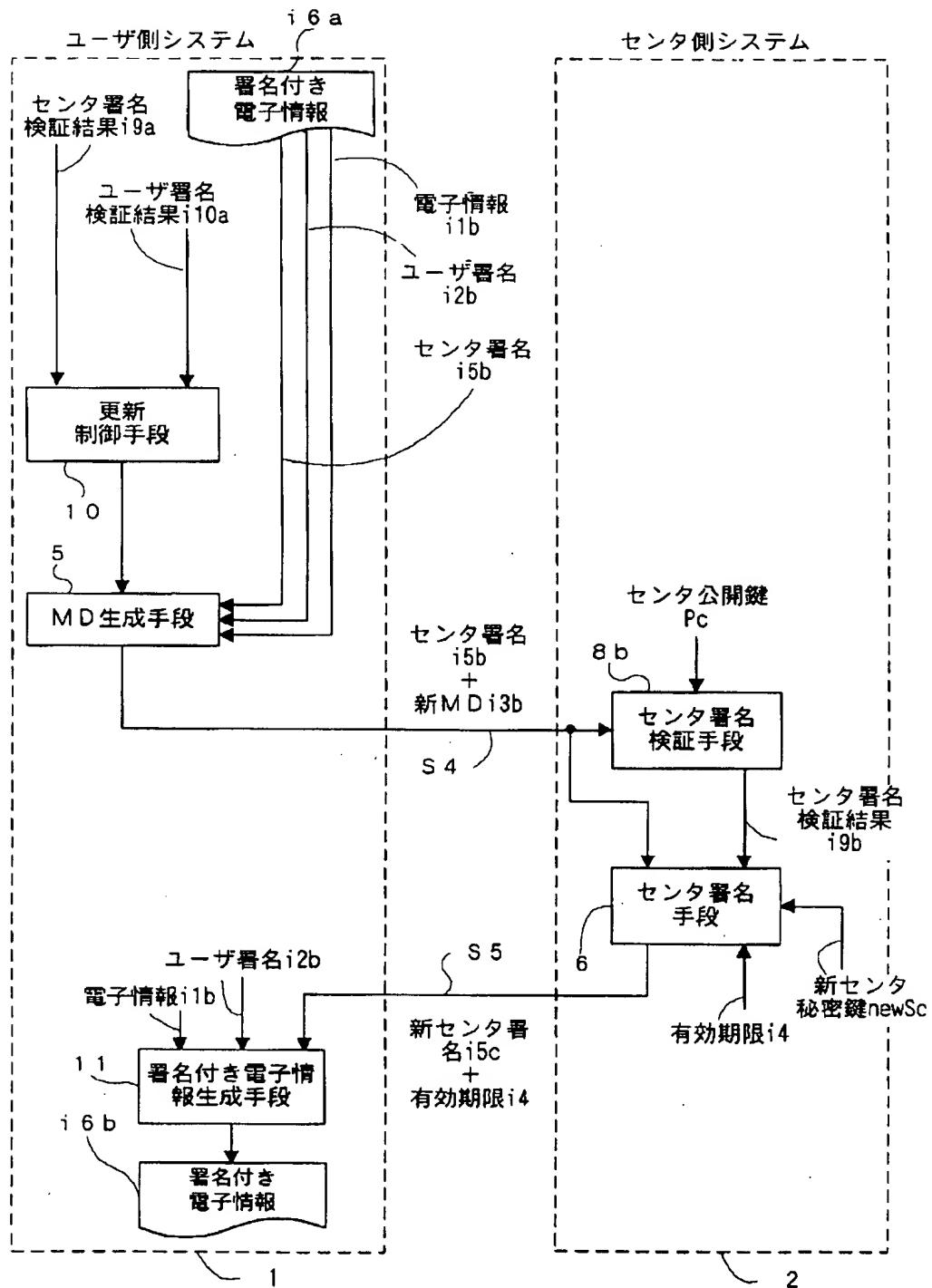
【図2】



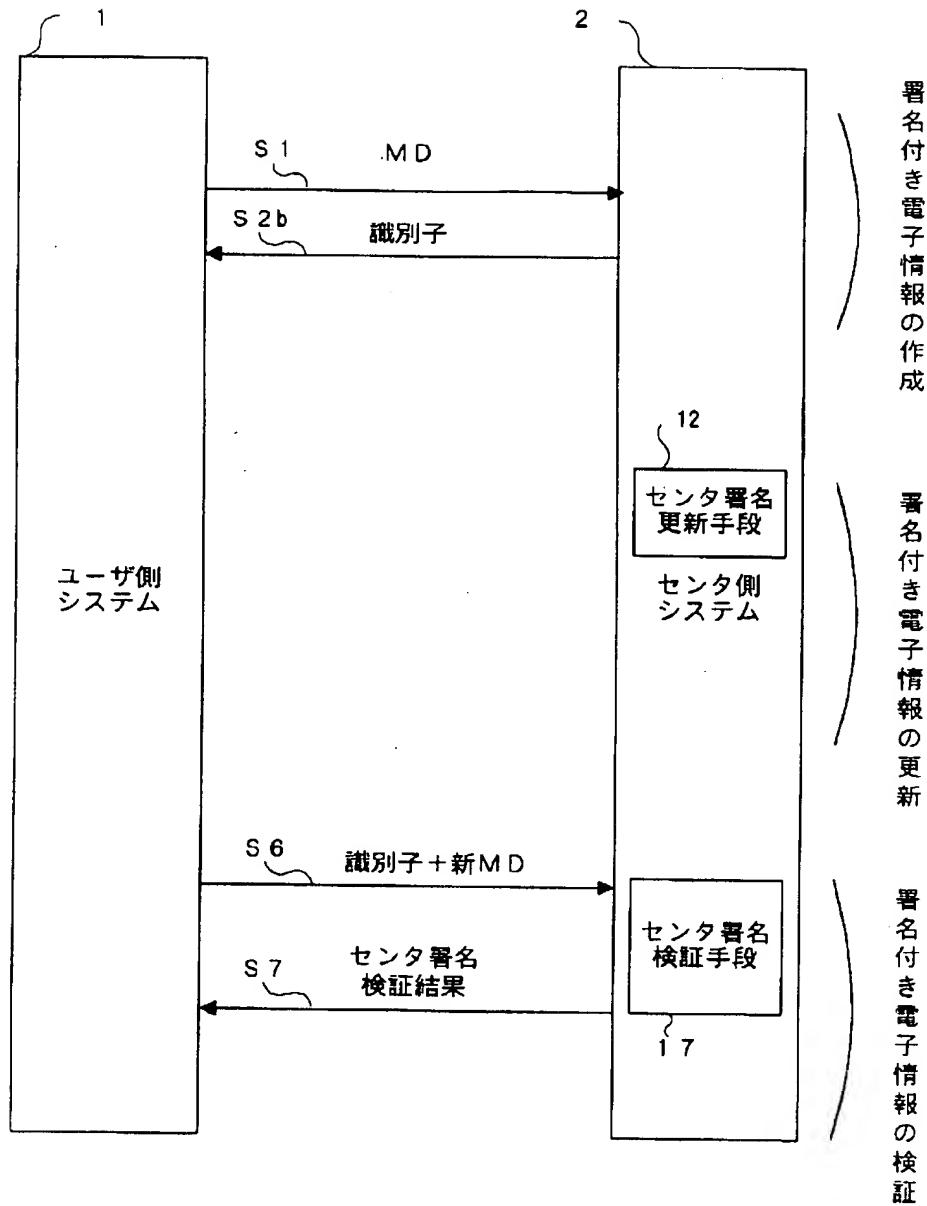
【図3】



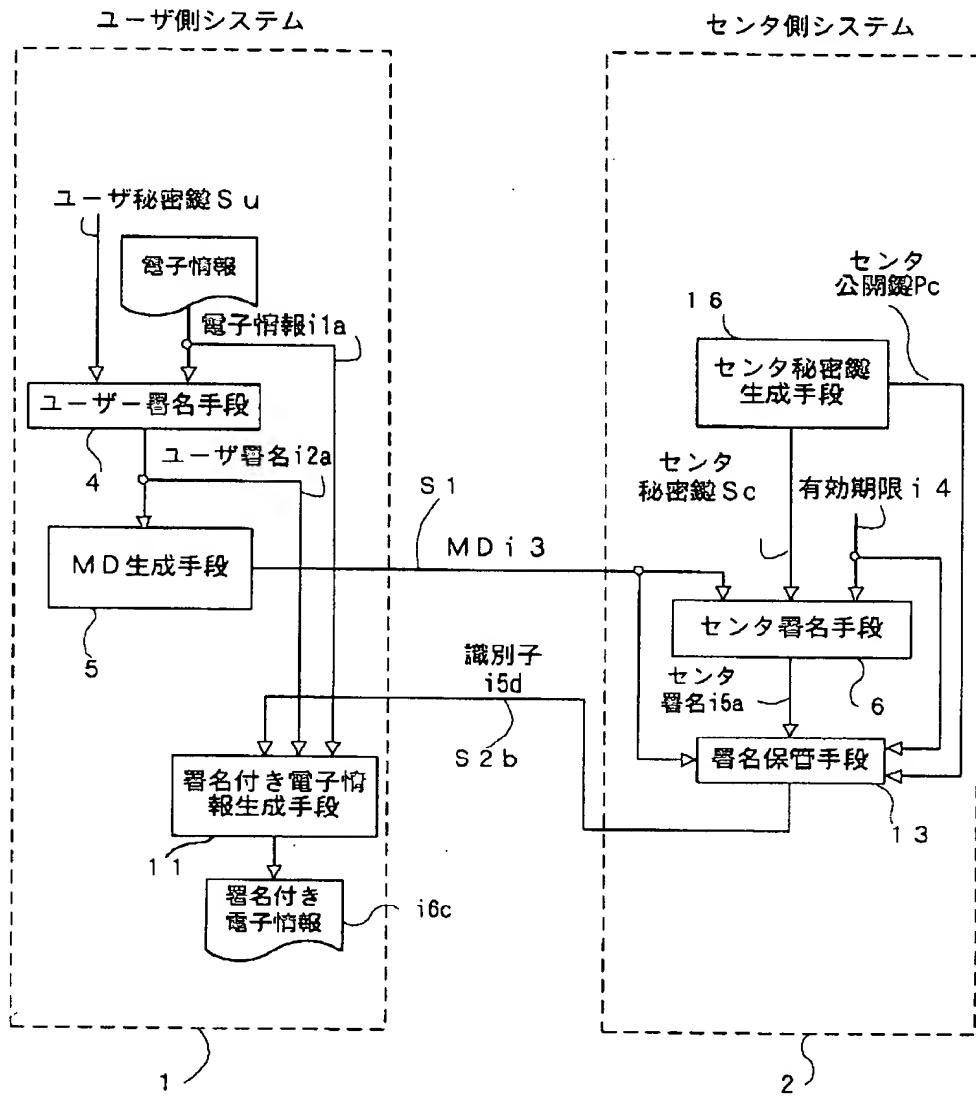
【図 4】



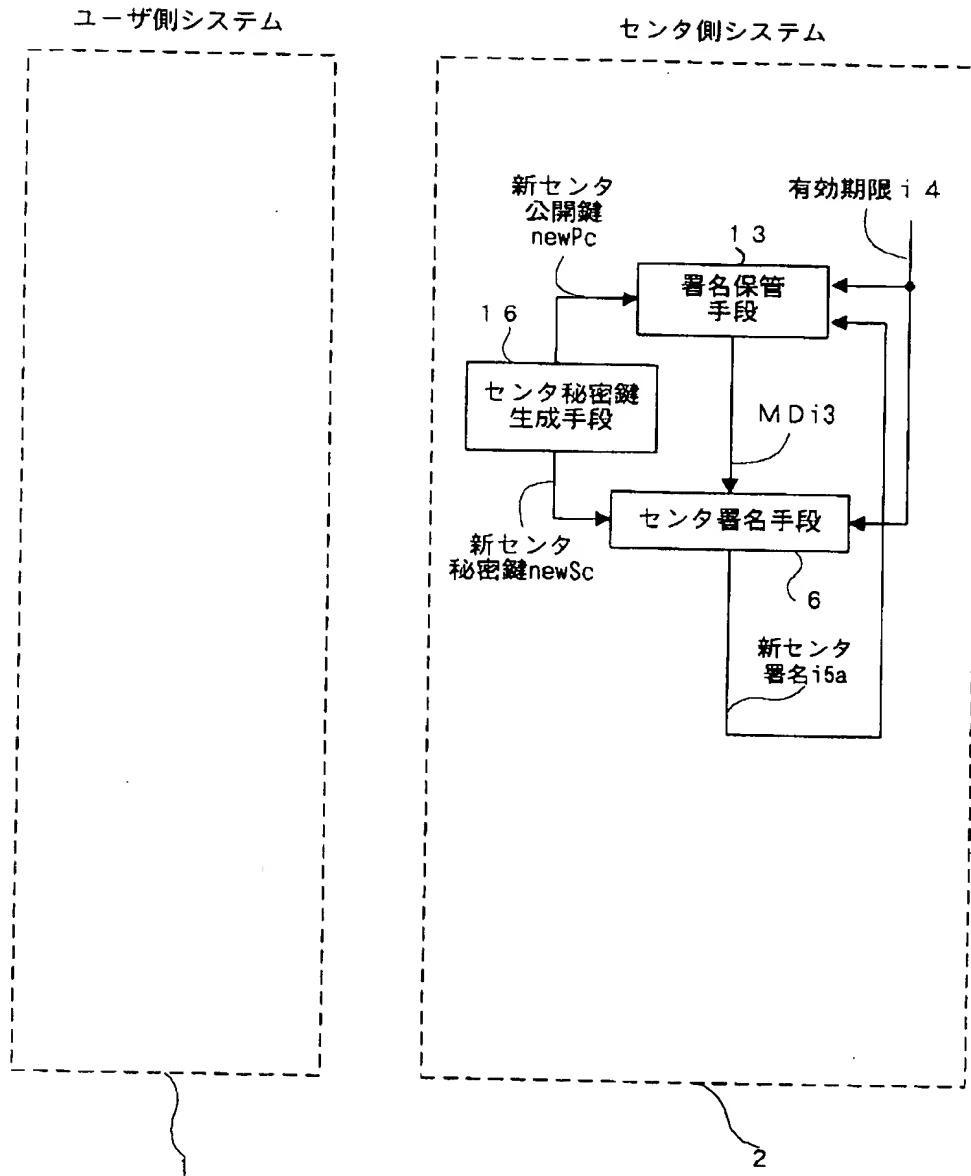
【図5】



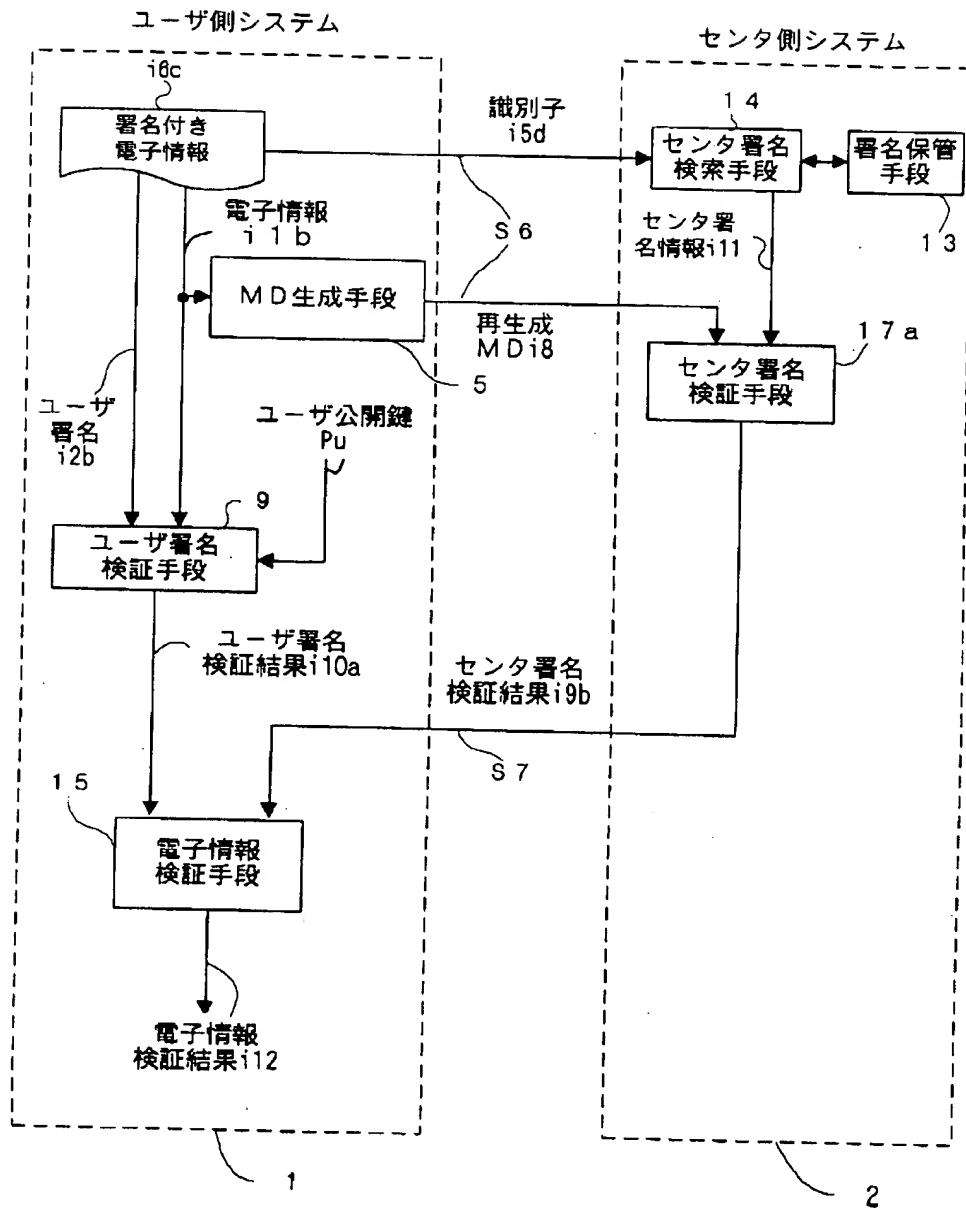
【图6】



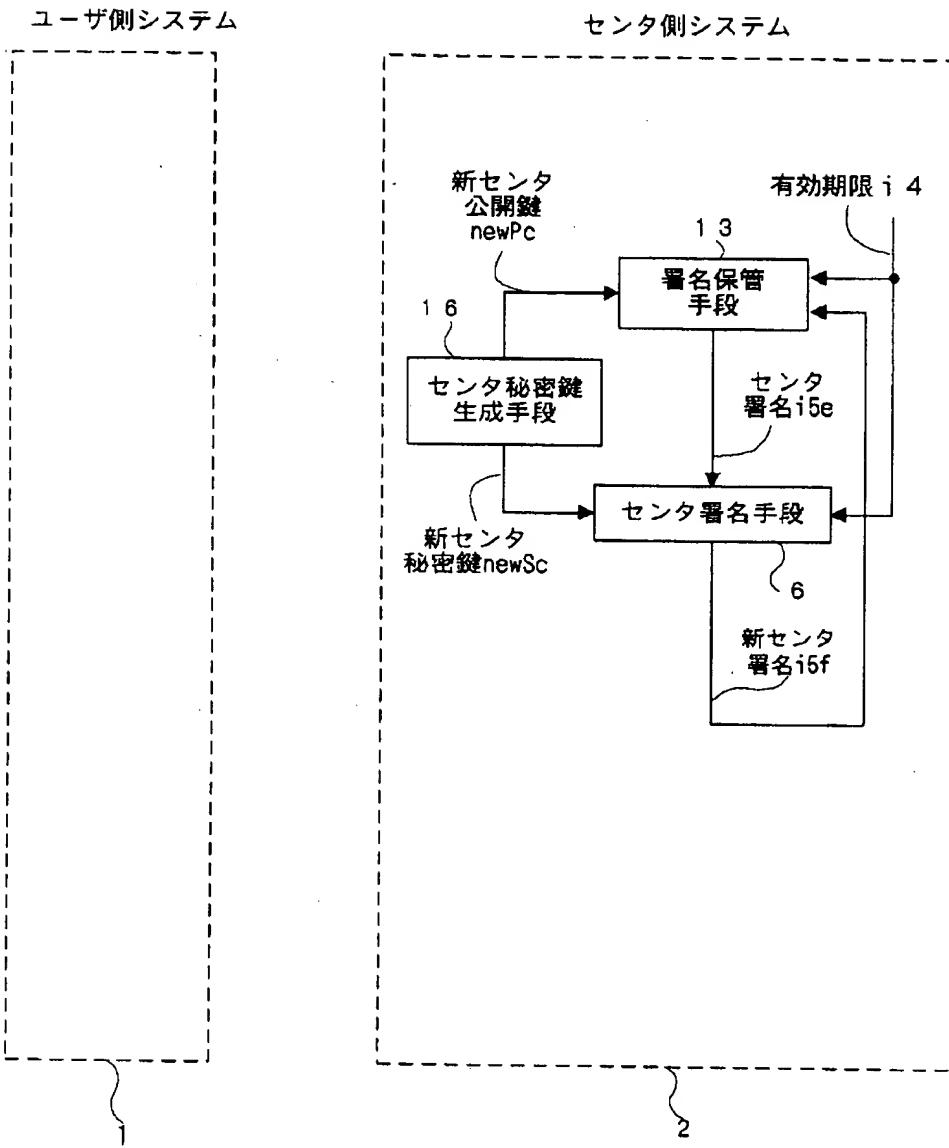
【図7】



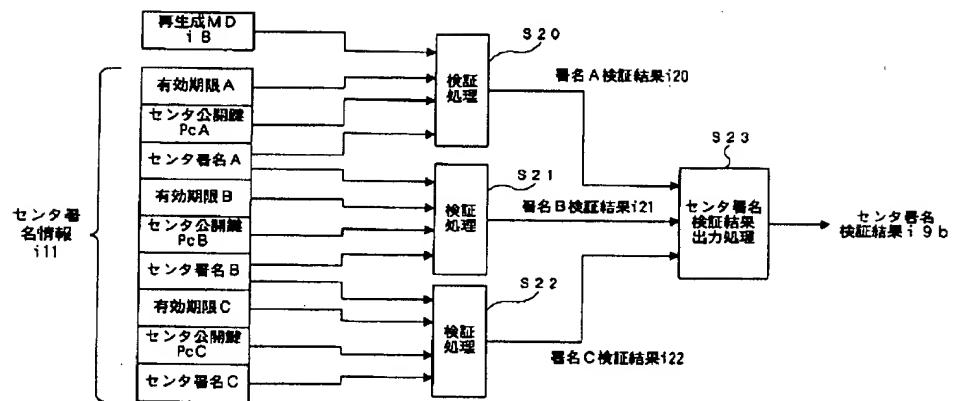
【図8】



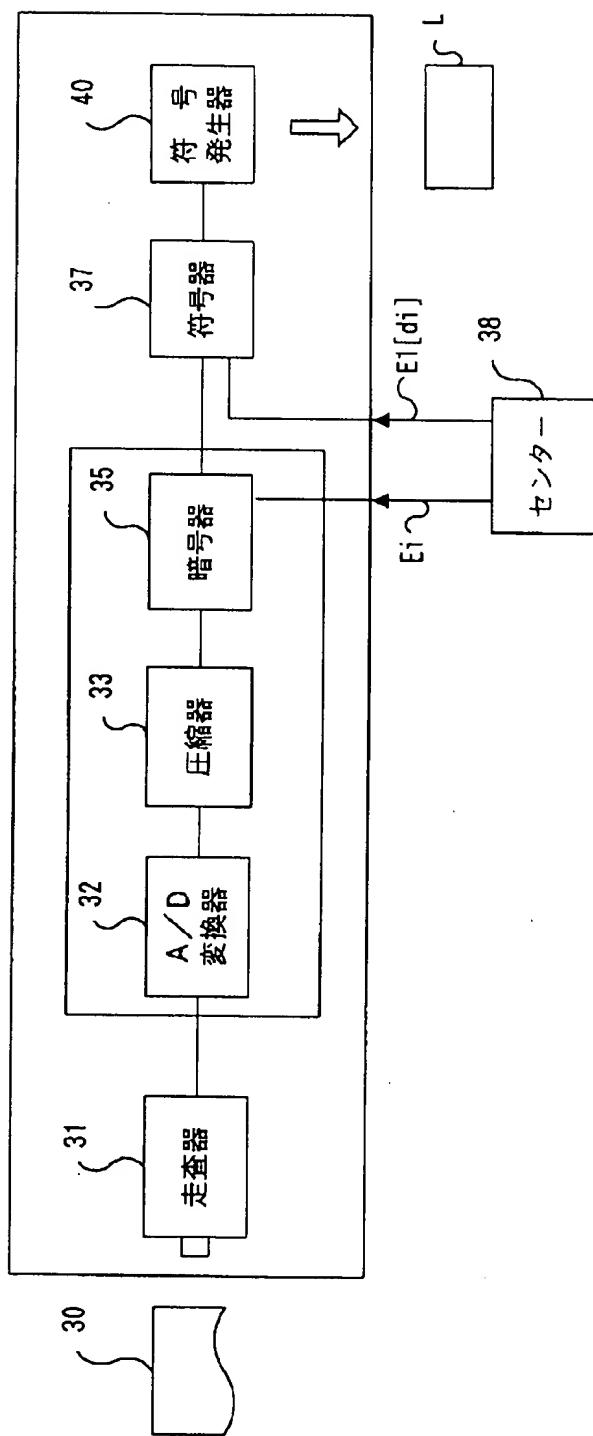
【図 10】



【図 1 1】



【図 12】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.